

An Online Decoding Schedule Generating Algorithm for Successive Cancellation Decoder of Polar Codes

Dan Le, Xiamu Niu*

The School of Computer Science and Technology, Harbin Institute of Technology, Harbin, 150001 China.

Abstract

Successive cancellation (SC) is the first and widely known decoder of polar codes, which has received a lot of attentions recently. However, its decoding schedule generating algorithms are still primitive, which are not only complex but also offline. This paper proposes a simple and online algorithm to generate the decoding schedule of SC decoder. Firstly, the dependencies among likelihood ratios (LR) are explored, which lead to the discovery of a sharing factor. Secondly, based on the online calculation of the sharing factor, the proposed algorithm is presented, which is neither based on the depth-first traversal of the scheduling tree nor based on the recursive construction. As shown by the comparisons among the proposed algorithm and existed algorithms, the proposed algorithm has advantages of the online feature and the far less memory taken by the decoding schedule.

Index Terms

Polar codes, successive cancellation decoder, decoding schedule, sharing factor

I. INTRODUCTION

Since Shannon presented the noisy channel coding theorem [1], polar code, introduced by Arikan [2], is the first class of codes achieving channel capacity with explicit construction. With the successive cancellation (SC) decoder, the channel capacity is asymptotically achieved by codelength N . Hence, polar codes have attracted many attentions recently[3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16].

As the first and widely known decoder of polar codes, a lot of research efforts have been made on SC decoder[6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. Some references focus on the simplified successive cancellation (SSC)[6], [8], [12], [13], [15], which simplifies the constituent code with rate zero in SC decoder. SSC can significantly reduce the decoding latency and implementation complexity of SC decoder, but its performance depends strongly on the underlying channel and it requires that all frozen bits must be zeros. However, in some scenarios, the frozen bits can not be zeros, for instance, the error reconciliation in the quantum key distribution[17], [18]. Since SC decoder asks no restrictions on the frozen bits and its performance does not rely on the underlying channel, lots of works[7], [10], [11], [14] are still done on the SC decoder. [7] presented an efficient hardware implementation of SC decoder with $O(N)$ processing elements and memory elements. [10] proposed a semi-parallel SC decoder for resource sharing and processor sharing at the cost of a small increase in decoding latency. [11] showed a look-ahead and overlapped architectures to decrease the decoding latency of SC decoder. [14] proposed an efficient partial sum network architecture to reduce the decoding latency and implementation complexity for semi-parallel SC decoder. Although so many works have been done on SC decoder, its decoding schedule generating algorithms are still primitive. As far as we know, there are just two existed decoding schedule generating algorithms. One is based on the depth-first traversal of the scheduling tree[6], [9], [12], [14], [15]. The other is based on the recursive construction[8]. However, the problems are that they not only are too complex, but also generate decoding schedule offline and store it in the ROM. To overcome the problems, based on the newly found factor z_i , this paper proposes a new algorithm to generate the decoding schedule of SC decoder. The presented algorithm is more simple, obtains the decoding schedule on the fly without introducing any extra delay, and decreases the memory storing the decoding schedule significantly. These advantages reduce the implementation complexity of SC decoder.

The remainder of this paper is organized as follows. In Section II we briefly review the SC decoder and introduce some notations. Section III explores the dependencies among likelihood ratios (LR), which lead to the discovery of the sharing factor z_i . Based on z_i , Section IV presents the proposed decoding schedule generating algorithm. Section V shows the comparisons among the proposed algorithm and existed algorithms. Finally, some conclusions are drawn in Section VI.

II. SC DECODER AND SOME NOTATIONS

First of all, let us list some notations used in this paper,

- $N = 2^n$ is the code length of polar code, and $n = \log_2 N$
- u_1^N is a shorthand for a row vector (u_1, \dots, u_N) , and u_i^j , $1 \leq i, j \leq N$, represents its subvector (u_i, \dots, u_j)
- $\{a, \dots, b\}$ represents the set of the integers ranging from a to b
- $\&$ is bitwise logical AND operator.

Polar codes take advantage of the polarization effect to achieve the channel capacity $I(W)$, whose channel model is illustrated as Figure 1, where u_1^N is the input vector, W_N is a combined channel by N independent copies of channel W , and y_1^N is the output vector with conditional probability $W_N(y_1^N | u_1^N)$. For the coordinate channels $W_N^{(i)}$ of W_N , the size of the set $\{W_N^{(i)} | I(W_N^{(i)}) \approx 1, 1 \leq i \leq N\}$ approaches $N \cdot I(W)$, while the size of the set $\{W_N^{(i)} | I(W_N^{(i)}) \approx 0, 1 \leq i \leq N\}$ approaches $N \cdot (1 - I(W))$. When sending data, only the good coordinate channels are employed, which are called information bits. The indices set of information bits are denoted as \mathcal{A} , whose size is denoted as K . The set of other indices is named as \mathcal{A}^c , on which the values are called frozen bits, denoted as $u_{\mathcal{A}^c} = (u_i | i \in \mathcal{A}^c)$. The frozen bits $u_{\mathcal{A}^c}$ are known by both sender and receiver. Hence polar codes are usually denoted as $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$.



Fig. 1. The illustration of the channel model of polar codes.

When decoding, SC decoder successively estimates the transmitted bits \hat{u}_1^N as follows,

$$\hat{u}_i = \begin{cases} u_i, & \text{if } i \in \mathcal{A}^c \\ 0, & \text{if } i \notin \mathcal{A}^c \text{ and } L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) \geq 1 \\ 1, & \text{if } i \notin \mathcal{A}^c \text{ and } L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) < 1 \end{cases} \quad (1)$$

, where

$$L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) = \frac{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | 0)}{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | 1)}. \quad (2)$$

(2) can be straightforwardly calculated using the recursive formula

$$L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) = \begin{cases} f\left(L_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1}), L_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, \hat{u}_{1,e}^{i-1})\right), & \text{when } i \text{ is odd} \quad (3a) \\ g\left(L_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1}), L_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, \hat{u}_{1,e}^{i-1}), \hat{u}_{i-1}\right), & \text{when } i \text{ is even} \quad (3b) \end{cases}$$

, where $f(a, b) = \frac{a \cdot b + 1}{a + b}$ and $g(a, b, s) = a^{1-2s} \cdot b$. We name $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$ as the i^{th} LR at length N . Its calculation is recursively converted into the calculations of the two LR at length $N/2$, and the recursion is continued down to the calculations of the N LR at length 1, i.e.

$$L_1^{(1)}(y_i) = \frac{W(y_i|0)}{W(y_i|1)}, \quad 1 \leq i \leq N, \quad (4)$$

which can be computed immediately according to the output vector y_1^N .

Another two recursive formulas similar to (3) are shown in (5) and (6), where $F(a, b) = 2\text{arctanh}(\tanh(a/2) \cdot \tanh(b/2))$, $G(a, b, s) = (-1)^s a + b$, and $\mathbb{F}(a, b) = \text{sgn}(a) \cdot \text{sgn}(b) \cdot \min\{|a|, |b|\}$. These two recursive formulas are both based on logarithm likelihood ratio (LLR), which is employed frequently by kinds of decoders, because it is always superior to the LR in terms of hardware utilization, computational complexity, and numerical stability[11]. (6) is also known as min-sum update rule, which further simplifies the implementations of the hyperbolic tangent function and its inverse function in (5). Although the recursive formulas (3), (5) and (6) are different, the dependencies among nodes are the same if we regard a LR or LLR as a node. Without loss of generality, we employ the recursive formula (3) to depict our idea.

$$\mathbb{L}_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) = \begin{cases} F\left(\mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1}), \mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, \hat{u}_{1,e}^{i-1})\right), & \text{when } i \text{ is odd} \quad (5a) \\ G\left(\mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1}), \mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, \hat{u}_{1,e}^{i-1}), \hat{u}_{i-1}\right), & \text{when } i \text{ is even} \quad (5b) \end{cases}$$

$$\mathbb{L}_N^{(i)}(y_1^N, \hat{u}_1^{i-1}) = \begin{cases} \mathbb{F}\left(\mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1}), \mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, \hat{u}_{1,e}^{i-1})\right), & \text{when } i \text{ is odd} \quad (6a) \\ G\left(\mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1}), \mathbb{L}_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, \hat{u}_{1,e}^{i-1}), \hat{u}_{i-1}\right), & \text{when } i \text{ is even} \quad (6b) \end{cases}$$

According to (1) and (3), in order to estimate \hat{u}_i , the computation of the i^{th} LR at length N is firstly activated, which in turn activates the two LR at length $N/2$. The two LR at length $N/2$ then activate the four LR at length $N/4$, which activate the eight LR at length $N/8$. The process continues till the LR at certain length, assumed as $N/2^k$, have been estimated. Then the computation is sequentially performed back from length $N/2^{k-1}$ to length N , and \hat{u}_i

is determined according to (1). In other words, SC decoder achieves the maximized sharing on the calculations of LR by a recursive way. We name the recursive way as implicitly maximized sharing, because it can not immediately recognize which of LR could be shared. To achieve an explicitly maximized sharing, the existed implementations firstly calculate the decoding schedule offline by certain algorithm, then store it in the ROM. Different from them, the proposed algorithm obtains the decoding schedule on the fly without introducing any extra delay, which owes to a new-found factor z_i .

III. DEPENDENCIES AMONG LRS

To achieve an explicitly maximized sharing on the calculations of LR, we firstly probe into the recursive formula (3) to explore the dependencies among LRs. It is obvious that there are three operations performing on the decoded bits \hat{u}_1^{i-1} in (3). They are the XOR between the subvectors with odd indices and even indices, the EXTRACTION of the subvector with even indices, and the EXTRACTION of the last element, i.e.

$$\begin{aligned} p(\hat{u}_1^{i-1}) &= \hat{u}_{1,o}^{i-1} \oplus \hat{u}_{1,e}^{i-1} = \hat{u}_{1,o}^{2\lfloor \frac{i-1}{2} \rfloor} \oplus \hat{u}_{1,e}^{2\lfloor \frac{i-1}{2} \rfloor} \\ q(\hat{u}_1^{i-1}) &= \hat{u}_{1,e}^{i-1} = \hat{u}_{1,e}^{2\lfloor \frac{i-1}{2} \rfloor} \\ r(\hat{u}_1^{i-1}) &= \hat{u}_{i-1}. \end{aligned} \quad (7)$$

By these three operations, we deduce which of LRs are used during the calculation of the i^{th} LR at length N .

Lemma 1 *For any given $1 \leq k \leq n$, the calculation of the i^{th} LR at length N , $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$, depends on the calculations of 2^k LRs at length $N/2^k$,*

$$L_{N/2^k}^{(\lceil i/2^k \rceil)} \left(y_{(j-1) \cdot N/2^k + 1}^{j \cdot N/2^k}, h_{j,k}(\hat{u}_1^{i-1}) \right), \quad 1 \leq j \leq 2^k, \quad (8)$$

where $h_{j,k}$ is a composite function of functions p and q . Specifically, $h_{j,k} = \theta_k \circ \theta_{k-1} \circ \dots \circ \theta_2 \circ \theta_1$, where

$$\theta_a = \begin{cases} p, & \text{when } b_{k-a+1} = 0 \\ q, & \text{when } b_{k-a+1} = 1 \end{cases}, \quad 1 \leq a \leq k, \quad (9)$$

and $b_k b_{k-1} \dots b_2 b_1$ is the binary expansion of the integer $j-1$.

Proof Please refer to Appendix I. □

(8) indicates that the LR_s at length $N/2^k$ depended by two diverse LR_s at length N are different in two items. One is $\lceil i/2^k \rceil$, and the other is $h_{j,k}(\hat{u}_1^{i-1})$. It is obvious that

$$\lceil i/2^k \rceil \equiv m, \text{ for } \forall (m-1)2^k + 1 \leq i \leq m2^k. \quad (10)$$

Then how about $h_{j,k}(\hat{u}_1^{i-1})$?

Lemma 2 For any given $1 \leq k \leq n$ and $1 \leq j \leq 2^k$, $h_{j,k}(\hat{u}_1^i)$ is a vector with the length of $\lfloor i/2^k \rfloor$, denoted as $(v_1, v_2, \dots, v_{\lfloor i/2^k \rfloor})$. Any element v_a is estimated as follows,

$$v_a = \bigoplus_{d \in D_{j,k,a}} \hat{u}_d, \quad 1 \leq a \leq \lfloor i/2^k \rfloor,$$

where

$$D_{j,k,a} = \{d \mid d = (a-1) \cdot 2^k + 1 + c_k c_{k-1} \cdots c_1\}, \quad (11)$$

$$c_t = \begin{cases} ?, & \text{when } b_{k-t+1} = 0 \\ 1, & \text{when } b_{k-t+1} = 1 \end{cases}, \quad 1 \leq t \leq k \quad (12)$$

$c_t = ?$ indicates that c_t can be 0 and 1, and $b_k b_{k-1} \cdots b_2 b_1$ is the binary expansion of the integer $j-1$.

Proof Please refer to Appendix II. □

Lema 2 shows that the vector $h_{j,k}(\hat{u}_1^{i-1})$ is determined by the values of j , k and $\lfloor (i-1)/2^k \rfloor$. Since $\lfloor (i-1)/2^k \rfloor \equiv m-1$ for all $(m-1)2^k + 1 \leq i \leq m2^k$, we have

$$h_{j,k}(\hat{u}_1^{i-1}) \equiv h_{j,k}(\hat{u}_1^{(m-1) \cdot 2^k}), \text{ for } \forall (m-1)2^k + 1 \leq i \leq m2^k. \quad (13)$$

Combining (10), (13) and Lema 1, it can be concluded that the 2^k LR_s at length N ,

$$L_N^{(i)}(y_1^N, \hat{u}_1^{i-1}), \quad (m-1)2^k + 1 \leq i \leq m2^k,$$

share the same 2^k LR_s at length $N/2^k$

$$L_{N/2^k}^{(m)} \left(y_{(j-1) \cdot N/2^k + 1}^{j \cdot N/2^k}, h_{j,k}(\hat{u}_1^{(m-1) \cdot 2^k}) \right), \quad 1 \leq j \leq 2^k. \quad (14)$$

According to the conclusion, we find a factor defined as Definition 1. It is the key to achieve an explicitly maximized sharing on the calculations of LR_s, as shown in the following Theorem 1.

Definition 1 (Sharing Factor) For any given $1 \leq i \leq N$, its sharing factor is denoted as z_i , which is the number of the consecutive zeros in the end of the binary expansion of the integer $i - 1$. It is noted that $z_i = n$ when $i = 1$.

In the view of the sharing factor z_i , $i - 1$ can be rewritten as follows,

$$i - 1 = \begin{cases} 0, & \text{if } i = 1 \\ m_o \cdot 2^{z_i}, & \text{otherwise} \end{cases} \quad (15)$$

where m_o is odd. Theorem 1 details the function of z_i on the explicitly maximized sharing on the calculations of LR_s.

Theorem 1 In SC decoder, when \hat{u}_i is estimated, only the LR_s at length $N, N/2, \dots, N/2^{z_i}$ should be calculated, while the LR_s at length $N/2^{z_i+1}, N/2^{z_i+2}, \dots, 1$ can be shared, where z_i is the sharing factor of i . Specifically, the calculations can be performed beginning with the LR_s at length $N/2^{z_i}$, and in sequence till ending with the LR at length N .

Proof Please refer to Appendix III. □

IV. PROPOSED DECODING SCHEDULE GENERATING ALGORITHM

For the estimation of \hat{u}_i , all required LR_s at length $N/2^k$ are listed in (14). Hence we just need to determine which of formula f and g is employed to calculate these LR_s. If the formula f is used, these calculations are denoted as $f_{N/2^k}$, otherwise denoted as $g_{N/2^k}$. For the sake of brevity, $f_{N/2^k}$ and $g_{N/2^k}$ are both represented by $\gamma_{N/2^k}$, then

$$\gamma_{N/2^k} = \begin{cases} f_{N/2^k}, & \text{when } \lceil i/2^k \rceil \text{ is odd} \\ g_{N/2^k}, & \text{when } \lceil i/2^k \rceil \text{ is even} \end{cases}. \quad (16)$$

According to Theorem 1, the decoding schedule for the estimation of \hat{u}_i is $\gamma_{N/2^{z_i}}, \gamma_{N/2^{z_i-1}}, \dots, \gamma_N$.

By employing the sharing factor z_i , we can further simplify the selection of $\gamma_{N/2^k}$ between $f_{N/2^k}$ and $g_{N/2^k}$. According to (15), we have

$$\lceil i/2^k \rceil = \begin{cases} \lceil 1/2^k \rceil, & \text{if } i = 1 \\ \lceil m_o \cdot 2^{z_i-k} + 1/2^k \rceil, & \text{otherwise} \end{cases},$$

where m_o is odd. Obviously, if $i = 1$, then $\lceil i/2^k \rceil$ is always equal to 1 for all the k , otherwise it is even for $k = z_i$ and odd for $k < z_i$. Here the case of $k > z_i$ are not considered, because

Theorem 1 shows that the LR_s at length $N/2^k$, $k > z_i$, can be shared and need not be calculated. Hence the parity of $\lceil i/2^k \rceil$ can be determined as follows,

$$\lceil i/2^k \rceil = \begin{cases} \text{even}, & \text{if } i \neq 1 \text{ and } k = z_i \\ \text{odd}, & \text{otherwise} \end{cases}, \quad (17)$$

and the selection of $\gamma_{N/2^k}$ can be rewritten as follows,

$$\gamma_{N/2^k} = \begin{cases} g_{N/2^k}, & \text{if } i \neq 1 \text{ and } k = z_i \\ f_{N/2^k}, & \text{otherwise} \end{cases}. \quad (18)$$

Another method to determine the selection of $\gamma_{N/2^k}$ was also presented in [10], [15], i.e.

$$\gamma_{N/2^k} = \begin{cases} g_{N/2^k}, & \text{when } (i-1) \& 2^k == 1 \\ f_{N/2^k}, & \text{when } (i-1) \& 2^k == 0 \end{cases}. \quad (19)$$

In their method, for each $1 \leq i \leq N$, the selections should be performed for all k . While our method shows that, for $2 \leq i \leq N$, the formula g is just employed one time, i.e. $k = z_i$, and for $i = 1$, the formula g does not be employed.

In a word, the proposed decoding schedule algorithm is summarized as follows. The SC decoder successively estimates the transmitted bits \hat{u}_1^N : for the estimation of \hat{u}_1 , $f_1, f_2, f_4, \dots, f_N$ are performed in sequence, and for the estimation of \hat{u}_i ($i > 1$), $g_{N/2^{z_i}}, f_{N/2^{z_i-1}}, \dots, f_N$ are performed in sequence. An example of $N = 8$ is shown in Table I. The first line is clock cycle, the second line is the entries of the decoding schedule, and the third line is the output of \hat{u}_i .

TABLE I
THE DECODING SCHEDULE OF SC DECODER FOR POLAR CODES WITH $N = 8$.

CC	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Entry	f_1	f_2	f_4	f_8	g_8	g_4	f_8	g_8	g_2	f_4	f_8	g_8	g_4	f_8	g_8
\hat{u}_i	N/A	N/A	N/A	\hat{u}_1	\hat{u}_2	N/A	\hat{u}_3	\hat{u}_4	N/A	N/A	\hat{u}_5	\hat{u}_6	N/A	\hat{u}_7	\hat{u}_8

In order to generate the decoding schedule online, we would like to calculate z_i on the fly. According to Bit Twiddling Hacks¹, the online calculation of z_i is feasible. An illustration with a multiply and a lookup table is shown in Algorithm 1. The algorithm works for any input $2 \leq i \leq 2^{32}$. For the case $i = 1$, z_1 is set to n . The codelength $N = 2^{32}$ is enough for almost

¹<http://graphics.stanford.edu/~seander/bithacks.html>.

all practical polar codes, whose codelengths usually are about 2^{20} bits. Since the calculation of z_i is so simple, its delay can be easily eliminated by packing it into the estimations of \hat{u}_j , ($j < i$). Hence z_i can be calculated on the fly without introducing any extra delay. The proposed algorithm thereby generates decoding schedule online without introducing any extra delay.

Algorithm 1 An illustration of calculating z_i

Input: i ;

Output: z_i ;

```

1: static const int LT[32] = { 0, 1, 28, 2, 29, 14, 24, 3, 30, 22, 20, 15, 25, 17, 4, 8, 31, 27,
    13, 23, 21, 19, 16, 7, 26, 12, 18, 6, 11, 5, 10, 9 };
2: int v = i - 1;
3:  $z_i = \text{LT}[(\text{uint32\_t})((v \& -v) * 0x077CB531)) >> 27]$ ;

```

V. COMPARISONS

To the best of our knowledge, there are two algorithms generating the decoding schedule of SC decoder, both of which calculate the decoding schedule offline and store it in the ROM. One is based on the depth-first traversal of the scheduling tree[6], [9], [12], [14], [15], as shown in Figure 2. The other is based on the recursive construction[8], as shown in Algorithm 2. Obviously, the proposed algorithm based on the sharing factor z_i is more simple.

Algorithm 2 Recursive-construction based decoding schedule generating algorithm[8]

Input: Codelength N ;

Output: Decoding schedule DS ;

```

1:  $DS = NULL$ ;
2: for  $i = n, i - -, 1$  do
3:    $DS1 = [f_{2^i}, DS]$ ;
4:    $DS2 = [g_{2^i}, DS]$ ;
5:    $DS = [DS1, DS2]$ ;
6: end for
7:  $DS = [f_1, DS]$ ;
8: Output  $DS$ ;

```

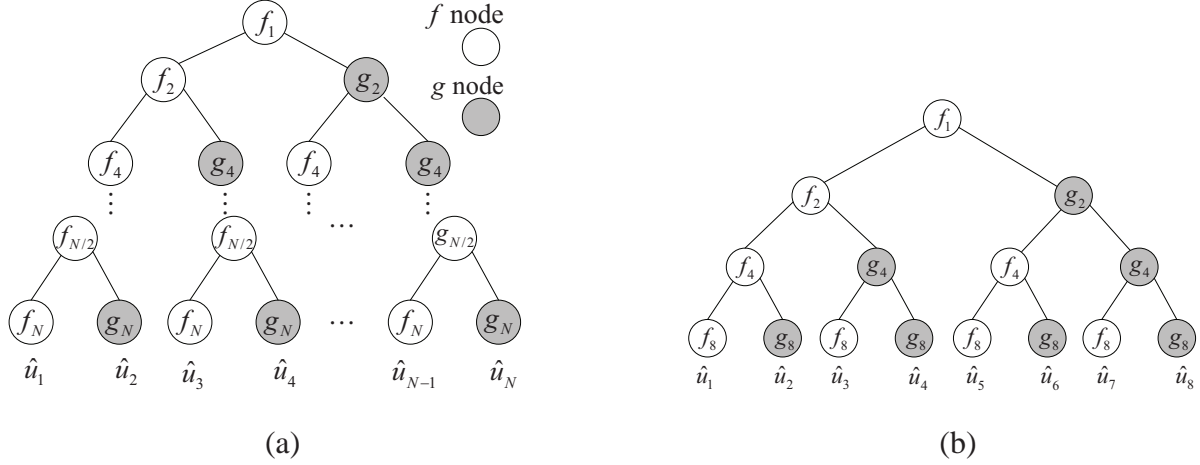


Fig. 2. Scheduling tree of the SC decoder for polar codes, whose depth-first traversal generates the decoding scheduling. (a) General scheduling tree. (b) Example of $N = 8$.

We compare the three algorithms in terms of online (No/Yes), extra delay(No/Yes), and memory. The indicator of online measures whether the decoding schedule is generated on the fly or not. The indicator of extra delay measures whether the generation of decoding schedule introduces extra delay into the decoding process. The indicator of memory shows the number of the storage taken by the decoding schedule. The comparison results are listed in Table II.

TABLE II
COMPARISONS AMONG DIFFERENT DECODING SCHEDULE GENERATING ALGORITHMS.

	Online	Extra Delay	Memory (bit)
Scheduling Tree[6], [9], [12], [14], [15]	No	No	$(2N - 1) \log_2 (2n + 1)$
Recursive Construction[8]	No	No	$(2N - 1) \log_2 (2n + 1)$
Proposed	Yes	No	160

Since the algorithms based on the scheduling tree and recursive construction both generate the decoding schedule offline and store it in the ROM, they are not online and do not introduce any extra delay. For the two existed algorithms, the required memory is equal to the product of the number of the entries of decoding schedule and the number of bits to represent each entry. It is obvious that the number of the entries of decoding schedule is the total nodes of schedule tree, i.e. $\sum_{k=0}^n 2^k = 2N - 1$. Each entry of decoding schedule can be represented at least by

$\log_2(2n+1)$, because there are $2n+1$ different entries, i.e. $f_1, \dots, f_{N/2}, f_N, g_2, \dots, g_{N/2}, g_N$. Hence the memory taken by the two existed algorithms are both $(2N-1)\log_2(2n+1)$. If Algorithm 1 is employed to calculate z_i , as mentioned above, the proposed algorithm can generate the decoding schedule on the fly without introducing any extra delay. Since only a lookup table needs to be stored during the running of the proposed algorithm, its required memory is constant, i.e. 160bits, which is far less than the memory taken by the two existed algorithms, especially for a large N . Usually, in order to achieve the channel capacity, the codelength of polar codes should be at least 2^{20} bits[10], [16], i.e. $N \geq 2^{20}$.

VI. CONCLUSIONS

Thanks to the new-found factor z_i , we have proposed a new decoding schedule generating algorithm, which is superior to the existed algorithms in two aspects. The first is that the existed algorithms are too complex, which are either based on the depth-first traversal of the scheduling tree or based on the recursive construction. While the proposed algorithm skillfully computes decoding schedule by the sharing factor z_i , which can be calculated easily with Bit Twiddling Hacks. The second is that the existed algorithms obtain decoding schedule offline and consume at least $(2N-1)\log_2(2n+1)$ bits to store it. While the proposed algorithm generates decoding schedule on the fly, and just requires 160 bits during the generation of the decoding schedule. These advantages are helpful to decrease the implementation complexity of SC decoder.

ACKNOWLEDGMENT

The authors gratefully acknowledge Wu Xianyan, Sang Jianzhi and Mao Haokun from Harbin Institute of Technology for many useful discussions on this paper. This work is supported by the National Natural Science Foundation of China (Grant Number: 61471141, 61361166006, 61301099) and the Fundamental Research Funds for the Central Universities (Grant Number: HIT. KISTP. 201416, HIT. KISTP. 201414).

APPENDIX I

PROOF OF LEMA 1

Proof

Basis Step: We start with the case $k = 1$. According to (3), the calculation of the i^{th} LR at length N , $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$, depends on the calculations of two LRs at length $N/2$ as follows,

$$L_{N/2}^{(\lceil i/2 \rceil)}(y_1^{N/2}, p(\hat{u}_1^{i-1})), \quad L_{N/2}^{(\lceil i/2 \rceil)}(y_{N/2+1}^N, q(\hat{u}_1^{i-1})).$$

Let $h_{1,1} = p$ and $h_{2,1} = q$, then the lema for the case $k = 1$ is true.

Inductive Step: Now we assume the truth of the case $k = m$. That is that the calculation of the i^{th} LR at length N depends on the calculations of 2^m LRs at length $N/2^m$ as follows,

$$L_{N/2^m}^{(\lceil i/2^m \rceil)}(y_{(j-1) \cdot N/2^m + 1}^{j \cdot N/2^m}, h_{j,m}(\hat{u}_1^{i-1})), \quad 1 \leq j \leq 2^m, \quad (20)$$

where

$$h_{j,m} = \theta_m \circ \theta_{m-1} \circ \dots \circ \theta_2 \circ \theta_1 \quad (21)$$

and

$$\theta_a = \begin{cases} p, & \text{when } b_{m-a+1} = 0 \\ q, & \text{when } b_{m-a+1} = 1 \end{cases}, \quad 1 \leq a \leq m. \quad (22)$$

Here $b_m b_{m-1} \dots b_2 b_1$ is the binary expansion of the integer $j - 1$. According to (3), if $\lceil i/2^m \rceil$ is odd, then each item in (20) is calculated as (23a), otherwise it is calculated as (23b).

$$L_{N/2^m}^{(\lceil i/2^m \rceil)}(y_{(j-1) \cdot N/2^m + 1}^{j \cdot N/2^m}, h_{j,m}(\hat{u}_1^{i-1})) = \begin{cases} f(\alpha, \beta), & \text{when } \lceil i/2^m \rceil \text{ is odd} \\ g(\alpha, \beta, r(h_{j,m}(\hat{u}_1^{i-1}))), & \text{when } \lceil i/2^m \rceil \text{ is even} \end{cases} \quad (23a)$$

where

$$\alpha = L_{N/2^{m+1}}^{(\lceil i/2^{m+1} \rceil)}(y_{(2j-2) \cdot N/2^{m+1} + 1}^{(2j-1) \cdot N/2^{m+1}}, p(h_{j,m}(\hat{u}_1^{i-1}))), \quad \beta = L_{N/2^{m+1}}^{(\lceil i/2^{m+1} \rceil)}(y_{(2j-1) \cdot N/2^{m+1} + 1}^{2j \cdot N/2^{m+1}}, q(h_{j,m}(\hat{u}_1^{i-1}))).$$

According to (23), It is obvious that the calculation of a LR at length $N/2^m$,

$$L_{N/2^m}^{(\lceil i/2^m \rceil)}(y_{(j-1) \cdot N/2^m + 1}^{j \cdot N/2^m}, h_{j,m}(\hat{u}_1^{i-1})),$$

depends on the calculations of two LRs at length $N/2^{m+1}$ as follows,

$$L_{N/2^{m+1}}^{(\lceil i/2^{m+1} \rceil)}(y_{(l-1) \cdot N/2^{m+1} + 1}^{l \cdot N/2^{m+1}}, h_{l,m+1}(\hat{u}_1^{i-1})), \quad l \in \{2j-1, 2j\}$$

, where

$$h_{l,m+1}(\hat{u}_1^{i-1}) = \begin{cases} p(h_{j,m}(\hat{u}_1^{i-1})), & \text{when } l = 2j-1 \\ q(h_{j,m}(\hat{u}_1^{i-1})), & \text{when } l = 2j \end{cases}. \quad (24)$$

That is

$$h_{l,m+1} = \begin{cases} p \circ f_m \circ \cdots \circ f_2 \circ f_1, & \text{when } l = 2j - 1 \\ q \circ f_m \circ \cdots \circ f_2 \circ f_1, & \text{when } l = 2j \end{cases}$$

Since $j \in \{1, 2, \dots, 2^m\}$, it can be inferred that $l \in \{1, 2, \dots, 2^{m+1}\}$ and

$$l - 1 = \begin{cases} b_m b_{m-1} \cdots b_1 0, & \text{when } l = 2j - 1 \\ b_m b_{m-1} \cdots b_1 1, & \text{when } l = 2j \end{cases}. \quad (25)$$

Hence the lema for the case $k = m + 1$ is true.

Consequently, by the Principle of Finite Induction, the lema is proved. \square

APPENDIX II

PROOF OF LEMA 2

Proof

Basis Step: We start with the case $k = 1$. In this case $j \in \{1, 2\}$, so we only need to consider $h_{1,1}(\hat{u}_1^i)$ and $h_{2,1}(\hat{u}_1^i)$. Since

$$\begin{aligned} h_{1,1}(\hat{u}_1^i) &= p(\hat{u}_1^i) = \hat{u}_{1,o}^{2[i/2]} \oplus \hat{u}_{1,e}^{2[i/2]}, \\ h_{2,1}(\hat{u}_1^i) &= q(\hat{u}_1^i) = \hat{u}_{1,e}^{2[i/2]}, \end{aligned} \quad (26)$$

it is obvious that their lengths are both $\lfloor i/2 \rfloor$. For any given $1 \leq a \leq \lfloor i/2 \rfloor$, we have

$$\begin{aligned} D_{1,1,a} &= \{2a - 1, 2a\} \\ &= \{d \mid d = (a - 1) \cdot 2 + 1 + ?\} \\ D_{2,1,a} &= \{2a\} \\ &= \{d \mid d = (a - 1) \cdot 2 + 1 + 1\}. \end{aligned}$$

Hence the lema for the case $k = 1$ is true.

Inductive Step: Now we assume the truth of the case $k = m$. Then we have

$$h_{j,m}(\hat{u}_1^i) = (v_1, v_2, \dots, v_{n_1}), \quad n_1 = \lfloor i/2^m \rfloor,$$

where $v_a = \bigoplus_{d \in D_{j,m,a}} \hat{u}_d$,

$$D_{j,m,a} = \{d \mid d = (a - 1) \cdot 2^m + 1 + c_m c_{m-1} \cdots c_1\},$$

$$c_t = \begin{cases} ?, & \text{when } b_{m-t+1} = 0 \\ 1, & \text{when } b_{m-t+1} = 1 \end{cases}, 1 \leq t \leq m,$$

and $b_m b_{m-1} \cdots b_2 b_1$ is the binary expansion of the integer $j - 1$.

(a) For any given $1 \leq l \leq 2^{m+1}$, when it is odd, according to (24) we have

$$h_{l,m+1}(\hat{u}_1^i) = p(v_1^{n_1}) = w_1^{n_2}.$$

Then $n_2 = \lfloor n_1/2 \rfloor = \lfloor i/2^{m+1} \rfloor$. For any element w_a , $1 \leq a \leq n_2$, we have

$$w_a = v_{2a-1} \oplus v_{2a} = \bigoplus_{d \in D_{j,m,2a-1} \cup D_{j,m,2a}} \hat{u}_d \stackrel{\Delta}{=} \bigoplus_{d \in D_{l,m+1,a}} \hat{u}_d$$

and

$$\begin{aligned} & D_{l,m+1,a} \\ = & D_{j,m,2a-1} \cup D_{j,m,2a} \\ = & \{d \mid d = (2a-2) \cdot 2^m + 1 + c_m c_{m-1} \cdots c_1\} \cup \{d \mid d = (2a-1) \cdot 2^m + 1 + c_m c_{m-1} \cdots c_1\} \\ = & \{d \mid d = (a-1) \cdot 2^{m+1} + 1 + 0 c_m c_{m-1} \cdots c_1\} \cup \{d \mid d = (a-1) \cdot 2^{m+1} + 1 + 1 c_m c_{m-1} \cdots c_1\} \\ = & \{d \mid d = (a-1) \cdot 2^{m+1} + 1 + ? c_m c_{m-1} \cdots c_1\}. \end{aligned}$$

Hence the lema for the case that $k = m + 1$ and l is odd is true.

(b) In a similar way, the case that $k = m + 1$ and l is even can also be proved.

Hence, combining (a) and (b), the lema is inferred to be true for the case $k = m + 1$.

Consequently, by the Principle of Finite Induction, the lema is proved. □

APPENDIX III

PROOF OF THEOREM 1

Proof According to (1), to estimate \hat{u}_i is to calculate the i^{th} LRs at length N , $L_N^{(i)}(y_1^N, \hat{u}_1^{i-1})$.

We firstly prove the proposition that the i^{th} and $(i-1)^{th}$ LR at length N can not share the same 2^k LRs at length $N/2^k$ if and only if there exists an integer m satisfying that $i-1 = m \cdot 2^k$. (i)

If there exists an integer m satisfying that $i-1 = m \cdot 2^k$, then

$$\begin{aligned} i-1 & \in \{(m-1) \cdot 2^k + 1, \dots, m \cdot 2^k\} \\ i & \in \{m \cdot 2^k + 1, \dots, (m+1) \cdot 2^k\} \end{aligned},$$

which means the $(i-1)^{th}$ and i^{th} LR at length N depend on two different groups of the 2^k LRs at length $N/2^k$. (ii) If there does not exists an integer m satisfying that $i-1 = m \cdot 2^k$, then

$i - 1$ is expressed as $i - 1 = a \cdot 2^k + b$ where a and b are both integers and $1 \leq b \leq 2^k - 1$. So

$$i - 1, i \in \{a \cdot 2^k + 1, \dots, (a + 1) \cdot 2^k\},$$

which means the $(i - 1)^{th}$ and i^{th} LR at length N depend on the same 2^k LR at length $N/2^k$.

Now we employ the newly proved proposition to show the truth of the theorem.

(a) If $i = 1$, then for all $0 \leq k \leq n = z_1$ there exists the integer 0 satisfying that $i - 1 = 0 \cdot 2^k$, which means in this case all the LR at all the lengths should be estimated. Since the 2^{z_1} LR at length 1 are channel LR, (4) indicates that they can be estimated immediately. Afterwards the LR at length $2, 4, \dots, N$ can be calculated in sequence according to (3).

(b) Otherwise, for any given integer $k > z_i$, it does not exist any integer m satisfying that $i - 1 = m \cdot 2^k$, which means that the i^{th} and $(i - 1)^{th}$ LR at length N share the same 2^k LR at length $N/2^k$ when $k > z_i$. On the other hand, for any given integer $k \leq z_i$, there exists the integer $m_i = 2^{z_i-k} m_o$ satisfying that $i - 1 = m_i \cdot 2^k$, which means that the i^{th} and $(i - 1)^{th}$ LR at length N can not share the same 2^k LR at length $N/2^k$ when $k \leq z_i$. Therefore only the LR at length $N, N/2, \dots, N/2^{z_i}$ should be calculated. Since the shared 2^{z_i+1} LR at length $N/2^{z_i+1}$ have been calculated during the estimation of \hat{u}_{i-1} ², the 2^{z_i} LR at length $N/2^{z_i}$ can be directly computed according to (3). Afterwards the LR at length $N/2^{z_i-1}, N/2^{z_i-2}, \dots, N$ can be calculated in sequence according to (3).

Combining **(a)** and **(b)**, the theorem is proved. \square

REFERENCES

- [1] C. E. Shannon, "A mathematical theory of communication," *The Bell Technical Journal*, vol. 27, no. 4, pp. 379–423, 1948.
- [2] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 3051–3073, 2009.
- [3] N. Hussami, S. B. Korada, and R. Urbanke, "Performance of polar codes for channel and source coding," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*. IEEE, 2009, pp. 1488–1492.
- [4] I. Tal and A. Vardy, "List decoding of polar codes," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 1–5.
- [5] K. Niu and K. Chen, "Stack decoding of polar codes," *Electronics letters*, vol. 48, no. 12, pp. 695–697, 2012.
- [6] A. Alamdar-Yazdi and F. R. Kschischang, "A simplified successive-cancellation decoder for polar codes," *IEEE communications letters*, vol. 15, no. 12, pp. 1378–1380, 2011.

²More precisely, the shared 2^{z_i+1} LR at length $N/2^{z_i+1}$ are either calculated during the estimation of \hat{u}_{i-1} , or also shared by \hat{u}_{i-1} and \hat{u}_{i-2} . In any case, the shared 2^{z_i+1} LR have already been calculated.

- [7] C. Leroux, I. Tal, A. Vardy, and W. J. Gross, "Hardware architectures for successive cancellation decoding of polar codes," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1665–1668.
- [8] Z. Chuan, Y. Bo, and K. K. Parhi, "Reduced-latency sc polar decoder architectures," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 3471–3475.
- [9] Z. Huang, C. Diao, and M. Chen, "Latency reduced method for modified successive cancellation decoding of polar codes," *Electronics letters*, vol. 48, no. 23, pp. 1505–1506, 2012.
- [10] C. Leroux, A. J. Raymond, G. Sarkis, and W. J. Gross, "A semi-parallel successive-cancellation decoder for polar codes," *Signal Processing, IEEE Transactions on*, vol. 61, no. 2, pp. 289–299, 2013.
- [11] C. Zhang and K. K. Parhi, "Low-latency sequential and overlapped architectures for successive cancellation polar decoder," *Signal Processing, IEEE Transactions on*, vol. 61, no. 10, pp. 2429–2441, 2013.
- [12] G. Sarkis and W. J. Gross, "Increasing the throughput of polar decoders," *Communications Letters, IEEE*, vol. 17, no. 4, pp. 725–728, 2013.
- [13] G. Sarkis, P. Giard, A. Vardy, C. Thibeault, and W. J. Gross, "Fast polar decoders: Algorithm and implementation," *Selected Areas in Communications, IEEE Journal on*, vol. 32, no. 5, pp. 946–957, 2014.
- [14] Y. Fan and C.-Y. Tsui, "An efficient partial-sum network architecture for semi-parallel polar codes decoder implementation," *Signal Processing, IEEE Transactions on*, vol. 62, no. 12, pp. 3165–3179, June 2014.
- [15] B. Le Gal, C. Leroux, and C. Jego, "Multi-gb/s software decoding of polar codes," *Signal Processing, IEEE Transactions on*, vol. 63, no. 2, pp. 349–359, 2015.
- [16] H. Yoo and I.-C. Park, "Partially parallel encoder architecture for long polar codes," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 62, no. 3, pp. 306–310, 2015.
- [17] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key reconciliation for high performance quantum key distribution," *Scientific reports*, vol. 3, 2013.
- [18] L. Qiong, L. Dan, M. Haokun, N. Xiamu, L. Tian, and G. Hong, "Study on error reconciliation in quantum key distribution," *Quantum Information & Computation*, vol. 14, no. 13-14, pp. 1117–1135, 2014.